

University of Alabama in Huntsville

LOUIS

Honors Capstone Projects and Theses

Honors College

4-22-2024

Escaping the Net: Detecting and Avoiding Phishing Attacks

Sarah Elizabeth Foltz

University of Alabama in Huntsville

Follow this and additional works at: <https://louis.uah.edu/honors-capstones>

Recommended Citation

Foltz, Sarah Elizabeth, "Escaping the Net: Detecting and Avoiding Phishing Attacks" (2024). *Honors Capstone Projects and Theses*. 884.

<https://louis.uah.edu/honors-capstones/884>

This Thesis is brought to you for free and open access by the Honors College at LOUIS. It has been accepted for inclusion in Honors Capstone Projects and Theses by an authorized administrator of LOUIS.

Escaping the Net: Detecting and Avoiding Phishing Attacks

by

Sarah Elizabeth Foltz

An Honors Capstone

submitted in partial fulfillment of the requirements

for the Honors Diploma

to

The Honors College

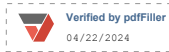
of

The University of Alabama in Huntsville

04/22/2024

Honors Capstone Project Director: Dr. Ivan Hovermale

Sarah Foltz



04/22/2024

Student

Date

Ivan D Hovermale Jr

Digitally signed by Ivan D Hovermale Jr
Date: 2024.04.15 14:23:04 -05'00'

Project Director

Date

Wai Yin Mok

Digitally signed by Wai Yin Mok
Date: 2024.04.22 15:02:31 -05'00'

Department Chair

Date

Honors College Dean

Date



Honors College

Frank Franz Hall

+1 (256) 824-6450 (voice)

+1 (256) 824-7339 (fax)

honors@uah.edu

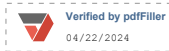
Honors Thesis Copyright Permission

This form must be signed by the student and submitted with the final manuscript.

In presenting this thesis in partial fulfillment of the requirements for Honors Diploma or Certificate from The University of Alabama in Huntsville, I agree that the Library of this University shall make it freely available for inspection. I further agree that permission for extensive copying for scholarly purposes may be granted by my advisor or, in his/her absence, by the Chair of the Department, Director of the Program, or the Dean of the Honors College. It is also understood that due recognition shall be given to me and to The University of Alabama in Huntsville in any scholarly use which may be made of any material in this thesis.

Student Name (printed)

Sarah Foltz



Student Signature

Date

Table of Contents

Cover Page	
Copyright	1
Table of Contents	2
Dedication	3
Abstraction	4
Method	5
Links	7
Phishing Slides	9
Vishing Slides	32
SMSishing Slides	43
Phishing Teaching Guide	54
Vishing Teaching Guide	57
SMSishing Teaching Guide	59
Assessment	61
Answer Key	64
Bibliography	67

Dedication:

This Capstone is dedicated to Elliot McKeel. I miss you, and wish you were here to graduate with me. You competed in CyberPatriot and STEM club events with me, and I would not be an IS major without these activities.

Thank you to my family, professors, mentors, and friends for helping me through life, college, and beyond.

Abstract:

This Honors Capstone describes the process of creating lesson plans for Alabama School of Cyber Technology and Engineering. These modules were created for the Social Engineering class and focus on phishing, vishing, and SMSishing. Inspiration for this class is from Dr. Hovermale's Social Engineering class.

Method:

I designed lesson plans and assessments about phishing, vishing, and SMSishing for this project, designed to be presented to Alabama School of Cyber Technology and Engineering (ASCTE) students in their Social Engineering Class. I chose this project because of my experience working as a Crew Trainer and Presenter at the US Space and Rocket Center and my experience in the Civil Air Patrol (CAP). I found a love for educating middle and high schoolers, and through these experiences, I discovered I enjoyed learning cybersecurity. I hope to volunteer with organizations that allow me to make a difference in the lives of young people.

I took a Social Engineering Class with Dr. Hovermale as a part of my Cybersecurity concentration. We worked together to come up with the idea to write modules for ASCTE's social engineering class.

I started this project by reaching out to Dr. Hovermale to be put in contact with the teacher of the Social Engineering class, Mr. Jamie Reese. I then contacted Mr. Reese to learn the class structure and his expectations for these modules. I also asked about how many days I should go and teach. He said he was hoping to cover three classes with that material. I explained what each module would include and began working on creating said modules. I also found out what standards Mr. Reese was attempting to cover, to ensure I understood why I was making these modules.

I then began designing these lessons. I modeled the lesson plan on my memories of classes in high school, how I taught at Space Camp, and how I taught at CAP days. I also considered what activities I had done in Dr. Hovermale's classes and what activities I had enjoyed in high school. I then designed three Google Slides presentations alongside Google Docs that could be used to teach. The slide presentations are used for showing to the class. The Google Docs ensures that even if I am not the one teaching these lessons, the presenter can recreate the stories I tell. In these lessons, I built in group activities, games, and homework assignments. The variety and repetition of this knowledge will help students learn the

information better. Hopefully, these activities will also engage the students and help them enjoy learning cybersecurity.

I decided that this project should be underwater-themed to play on the phishing/fishing pun, hoping to make the modules more engaging. I used information learned in my Social Engineering Class with Dr. Hovermale to design the content for this class. In these modules, I attempted to work with real examples that my family, friends, and I received to show students how often Phishing, Vishing, and SMSishing attacks occur. Using actual instances helps students understand the prevalence and format of these attacks. In my presentation, I also highlight how to spot these attacks, the dangers of these attacks, and how to report these attacks.

I sent rough and final drafts of each presentation to Mr. Reese and Dr. Hovermale for approval and suggestions. I implemented suggestions and finished writing toward the end of the fall 2023 semester. Over the break, I began writing an assessment for all three presentations that could be used as quizzes or tests. I included multiple-choice, written, and true/false questions. I also wrote an answer key for this assessment. I planned to present these lessons to the students in the spring 2024 semester. However, scheduling and security issues sadly made this impossible.

The slide sets, teaching guides, assessment, and answer key, as well as links to these documents, follow.

Links:

Phishing Slide set:

https://docs.google.com/presentation/d/1KqiLvfhRX8rCw1VEKHIPC6XGFrJ0mTh4KrNuR7hel0/edit?usp=drive_link

Vishing Slide set:

https://docs.google.com/presentation/d/1TxqTSbPQue6d7_yGhQURZScBBRdT2U3wnKdrwXRox80/edit?usp=drive_link

SMSishing Slide set:

https://docs.google.com/presentation/d/1HDEtz1N_vcWXm9GsRiQuVRf7ZCKu5KXxfVIIAIM344Y/edit?usp=drive_link

Phishing teaching guide: [https://docs.google.com/document/d/1aLmOC-](https://docs.google.com/document/d/1aLmOC-r474LFeH44Lc0Ga8dt9PZ8vC6rZDzN57n97Gw/edit?usp=drive_link)

[r474LFeH44Lc0Ga8dt9PZ8vC6rZDzN57n97Gw/edit?usp=drive_link](https://docs.google.com/document/d/1aLmOC-r474LFeH44Lc0Ga8dt9PZ8vC6rZDzN57n97Gw/edit?usp=drive_link)

Vishing teaching guide:

https://docs.google.com/document/d/19yCH_1Vw4WMSHsIpNZsyLqFa93LPsfWj5ou0h-H1-J0/edit?usp=drive_link

SMSishing teaching guide:

https://docs.google.com/document/d/1T6xTTgYM6g6eIxzEam3nTOalMovaba2Eac5pSYj3iY/e-dit?usp=drive_link

Assessment:

https://docs.google.com/document/d/1dHx8v4V_sPMeei2B1T3nGQ9GsaMeUH4t3EgPN-VcNXI/edit?usp=drive_link

Answer key:

https://docs.google.com/document/d/1nq05cjb2HwuatDjEfiWf-3K479ai-NVILKLv6u0Pab4/edit?usp=drive_link

Phishing Slide Deck:

What is Phishing?

On a sheet of paper,
describe phishing in a few
sentences.

An Introduction To ***PHISHING*** **In Social Engineering**





What is Phishing?



What is Phishing?

Are we talking about fish?

What is Phishing?

Are we talking about fish?

NO!

PHISHING is...

when fraudulent emails from seemingly-reputable companies or people ask for Personally Identifiable Information (PII) for nefarious purposes or try and convince users to click a link or download an attachment that installs malware.

PHISHING is...



when fraudulent emails from seemingly-reputable companies or people who ask for Personally Identifiable Information (PII) for nefarious purposes

Examples of Personally Identifiable Information

Examples of Personally Identifiable Information

- Name
- Address
- Email
- Phone number
- Date of Birth
- Passport Number
- Social Security Number
- Credit Card Number
- Fingerprint data
- Drivers License Number

Phishing in Social Engineering



What is Social Engineering?

Phishing in Social Engineering

*How is
phishing
related?*

Examples of Phishing



From: **Lourdes Valentina GAROF...** >
October 31, 2023 at 23:45

[External] VIRTUAL ADMINISTRATIVE ASSISTANT EMPLOYMENT FOR STUDENTS

Dear students...

Streamline your work schedule and earn \$450 a week. It's flexible. Part-time job. Home and campus are both used for all tasks. A job where you You don't need to travel anywhere, and you don't need to have a car to get Started. Please find the position and some basic information below.

Position Type: Part-Time Job Position (REMOTELY)
During this time, working from home would be very convenient. Consequently, you have been offered a campus administration or executive position. An assistant is needed for a data entry position.

This is a DATA ENTRY position, and no skills are needed for this position. The opportunity will be taught from the comfort of your home or via the internet. This will not affect your studies...

For more information, please send your full name and phone number for review and interview to the following email address: dr.suzannegeorgee02@gmail.com

Position: Executive Assistant/Bookkeeper For Students (REMOTELY)!!!
2-4 days a week
Pay Rate: \$450 weekly

Examples of Phishing

[External] STUDY OPPORTUNITY External Spam x

Dr.Professor Fedrich Frobel <richard13416@gmail.com>
to daniel.hall, darlene.showalter, darryl.walker, debbie.allen, Diane.aloisio, eduardo.valladares, erlan.waldron, et

Why is this message in spam? It is similar to messages that were identified as spam in the past.

Report not spam

Hello Student,

I am Dr.Professor Fedrich Frobel and I work as a Clinical Counsellor for the Department of Disability of United Nations Central Emergency Response Fund Secretariat (UNCERF) I provide individual and group therapy, coaching, assessment, and academic screenings to support students with disabilities (Physical, Chronic, Psychiatric, & Invisible) registered with (UNCERF). You have received this email because you have an offer from the University Office for able Students to work with me while we help students with disabilities frustrated with ignorance and lack of services as my temporary personal assistant. My present daily busy schedule demands the role of someone who is trustworthy, someone who will help support my work load when I am not in the United States in order for me to establish timely delivery of services and attend to important matters.

The sensitivity of this position warrants the office holder to be upright, responsive, accountable, trustworthy, emphatic, persevering and honest. This is a very simple job. You will only help me purchase some items and important matters when needed. This employment only takes an hour a day and 3 times a week for (1,500 dollars) weekly.

I am unable to meet up for an interview because I am currently away and helping the disabled students in Australia. You will be paid in advance for all tasks and purchased to be done on my behalf. Upon my arrival we will discuss the possibility of making this a long-term employment if I am impressed with your services while I am away. My arrival is scheduled for two weeks from now. I got your email through a short list from the Human Resources department to give out jobs to a few students in your university.

Do confirm acceptance of this position if you are interested in moving forward kindly, please provide or fill in the below form

Full names:

DOB:

Address:

Cell Number:

WhatsApp number:

Google chat email:

Alternate Email (different from school email):

I await your positive response
Sincerely,
Dr.Professor Fedrich Frobel
Professor Humanitarian Relief
E-mail fedrichfrobel@gmail.com

NOTE: THIS IS STRICTLY A WORK ONLINE FROM HOME POSITION

Regards
UNCERF Career Opportunity

Examples of Phishing

(More) Examples of Phishing

University Phish Bowls also have examples. For example:

<https://it.cornell.edu/phish-bowl>



Spear Phishing & Whaling



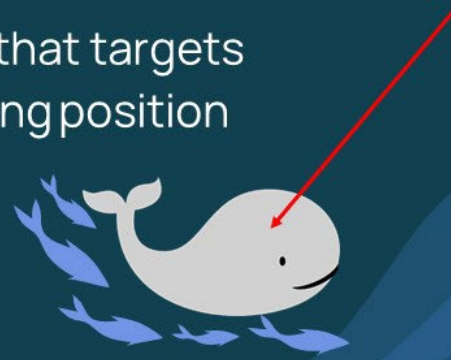
SPEAR PHISHING is...

a phishing attack that targets a specific person



WHALING is...

a spear phishing attack that targets someone in a high-ranking position of authority



How Do You Identify Phishing Emails?

- Fake logos
- Wrong email addresses
- Does not make sense for this person to email you
- Tries to make you click a link
- Typos and spelling errors
- False urgency
- Addresses you by email or general term, not name
- Suspicious attachments
- Asking for PII

How Do You Identify Phishing Emails?

- Fake logos
- Wrong email addresses
- Does not make sense for this person to email you
- Tries to make you click a link
- Typos and spelling errors
- False urgency
- Addresses you by email or general term, not name
- Suspicious attachments
- Asking for PII

LG From: **Lourdes Valentina GAROF..** >
October 31, 2023 at 23:45

[External] VIRTUAL ADMINISTRATIVE ASSISTANT EMPLOYMENT FOR STUDENTS

Dear students...

Streamline your work schedule and earn **\$450 a week**. It's flexible. Part-time job. Home and campus are both used for all tasks. A job where **you You** don't need to travel anywhere, and you don't need to have a car to get Started. Please find the position and some basic information below.

Position Type: Part-Time Job Position (REMOTELY)
During this time, working from home would be very convenient. Consequently, you have been offered a **campus administration or executive position**. An assistant is needed for a data entry position.

This is a DATA ENTRY position, and no skills are needed for this position. The opportunity will be taught from the comfort of your home or via the internet. This will not affect your studies...

For more information, please send your full name and phone number for review and Interview to the following email address: **dr.suzannegeorgee02@gmail.com**

Position: **Executive Assistant/Bookkeeper** For Students (REMOTELY)!!!
2-4 days a week
Pay Rate: \$450 weekly

Examples of Phishing

[External] STUDY OPPORTUNITY External Spam x

Dr.Professor Fedrich Frobel <richard13416@gmail.com>
to daniel.hall, darlene.showalter, darryl.walker, debbie.allen, Diane.alotko, eduardo.valladares, erlan.waldron, et

Why is this message in spam? It is similar to messages that were identified as spam in the past.
Report not spam

Hello Student,

I am Dr.Professor Fedrich Frobel and I work as a Clinical Counsellor for the Department of Disability of United Nations Central Emergency Response Fund Secretariat (UNCERF) I provide individual and group therapy, coaching, assessment, and academic screenings to support students with disabilities (Physical, Chronic, Psychiatric, & Invisible) registered with (UNCERF). You have received this email because you have an offer from the University Office for able Students to work with me while we help students with disabilities frustrated with ignorance and lack of services as my temporary personal assistant. My present daily busy schedule demands the role of someone who is trustworthy, someone who will help support my work load when I am not in the United States in order for me to establish timely delivery of services and attend to important matters.

The sensitivity of this position warrants the office holder to be upright, responsive, accountable, trustworthy, emphatic, persevering and honest. This is a very simple job. You will only help me purchase some items and important matters when needed. This employment only takes an hour a day and 3 times a week for (**1,500 dollars**) weekly.

I am unable to meet up for an interview because I am currently away and helping the disabled students in Australia. **You will be paid in advance** for all tasks and purchased to be done on my behalf. Upon my arrival we will discuss the possibility of making this a long-term employment if I am impressed with your services while I am away. My arrival is scheduled for two weeks from now. I got your email through a short list from the Human Resources department to give out jobs to a few students in your university.

Do confirm acceptance of this position if you are interested in moving forward kindly, please provide or fill in the below form

Full names: _____
DOB: _____
Address: _____
Cell Number: _____
WhatsApp number: _____
Google chat email: _____
Alternate Email (different from school email): _____

I await your positive response
Sincerely,
Dr.Professor Fedrich Frobel
Professor Humanitarian Relief
E-mail fedrichfrobels@gmail.com

NOTE: THIS IS STRICTLY A WORK ONLINE FROM HOME POSITION

Regards
UNCERF Career Opportunity

Examples of Phishing



IS IT PHISHING?

From: Walmart <info@alumni.hd.swipeplanning.shop>

Date: November 4, 2023 at 8:08:19 PM CDT

Subject: Congrats laura

---W--Nb--D Bonjour fyxgvh arqxvs, ¡Gracias por suscribirte! | Thanks for subscribing! | Merci pour votre subscription! Oui, inscris moi sur cette liste. Merci de l'intérêt que vous portez à notre contenu ! Cliquez sur le bouton pour confirmer votre inscription à la newsletter Easyismvkv. Nous vous remercions de votre confiance. activation de compte sur Inscription-Facile Votre compte a été créé, mais il doit encore être activé.

Thanks for asking. There's a "forgot password" link on the login screen in the app. (see image beside when login).

In addition to that, there are a couple other options on the web (but not in the app):

Please Reset Your Password For your security, we are strengthening our password requirements and as a result, your existing password has been disabled

Please enter your email and click "Continue" below to send a password reset message to the email associated with your account. This email will contain a link to reset your password that will expire within 24 hours.

----m4cuLXHz;WZTxoZ----yo15Oqxp;UoSLmt ----
SwH5mHZD;AGvYrZ----PgNudJVv;keYHWn

Thanks for signing up to receive emails from the Children's Museum of Phoenix. Now you won't miss out on our special events, programs, discounts and so much more!

INSCRIPTIONS 2018-2019 Publié le 2 septembre 2018 par joel
Bonjour, Le processus d'inscription se modernise, car nous avons mis en place cette année un site WEB vous permettant de réaliser cette opération depuis chez vous à partir du lien situé en bas de ce message. Cependant, si vous rencontrez des difficultés, des permanences sont mises en places au gymnase Henri Barbusse, tous les soirs de 17h00 à 19h00 pour vous aider en cas de besoin, pour faire votre inscription en ligne.

IS IT PHISHING?



From: Walmart <info@alumni.hd.swipeplanning.shop>
Date: November 4, 2023 at 8:08:19 PM CDT
Subject: Congrats laura

---W--Nb-- D Bonjour fyxgvh arqxs, ¡Gracias por suscribirte! |
Thanks for subscribing! | Merci pour votre subscription! Oui, inscris
moi sur cette liste. Merci de l'intérêt que vous portez à notre
contenu ! Cliquez sur le bouton pour confirmer votre inscription à la
newsletter Easyismvk. Nous vous remercions de votre confiance.
activation de compte sur Inscription-Facile Votre compte a été créé,
mais il doit encore être activé.

Thanks for asking. There's a "forgot password" link on the login
screen in the app. (see image beside when login).

In addition to that, there are a couple other options on the web (but
not in the app):

Please Reset Your Password For your security, we are
strengthening our password requirements and as a result, your
existing password has been disabled.

and click "Continue" below to send a
message to the email associated with your account.
contain a link to reset your password that will expire
24 hours.

-----m4cuLXHz;WZTxoZ-----yo15Oqxp;UoSLmt ----
SwH5mHZD;AGvYrZ-----PgNudJVv;keYHWn

Thanks for signing up to receive emails from the Children's Museum
of Phoenix. Now you won't miss out on our special events,
programs, discounts and so much more!

INSCRIPTIONS 2018-2019 Publié le 2 septembre 2018 par joel
Bonjour, Le processus d'inscription se modernise, car nous avons
mis en place cette année un site WEB vous permettant de réaliser
cette opération depuis chez vous à partir du lien situé en bas de ce
message. Cependant, si vous rencontrez des difficultés, des
permanences sont mises en places au gymnase Henri Barbusse,
tous les soirs de 17h00 à 19h00 pour vous aider en cas de besoin,
pour faire votre inscription en ligne.

IS IT PHISHING?



UAH Green Club <greenclub@uah.edu>
9/19/2023 4:26 PM



[REDACTED]

WE'RE GOING HIKING!!

On Sunday, 9/24 the Green Club will be hiking the Lost Sink Trail at Keel Mountain Preserve to get
to know each other and learn about North Alabama's beautiful ecosystems and wildlife. The route
is moderately challenging.

Please arrive at the Charger Union lobby at 9:15 to meet for carpooling, to depart at 9:30. We
should arrive at Keel Mtn Preserve 1787 McMullen Rd, Gurley, AL 35748 at 10 AM.

If there are thunderstorms or the chance of rain exceeds 50% for the duration of the hike (10am-
12pm) we will cancel and try again the following Sunday at the same time/place.

We will also be meeting once again the day after, 9/25, from 6-7 in MOR 145 where the topic will
be Invasive Species.

Finally, on Sunday 10/15, we may be partnering with the Rock Climbing Club to help clean up the
bouldering area at Rainbow Mountain, which also has some nice hiking.

I hope to see you there!!



IS IT PHISHING?



UAH Green Club <greenclub@uah.edu>
9/19/2023 4:26 PM

[Redacted]

WE'RE GOING HIKING!!

On Sunday, 9/24 the Green Club will be hiking the Lost Sink Trail at Keel Mountain Preserve to get to know each other and learn about North Alabama's beautiful ecosystems and wildlife. The route is moderately challenging.

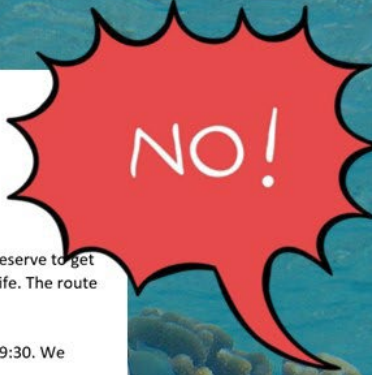
Please arrive at the Charger Union lobby at 9:15 to meet for carpooling, to depart at 9:30. We should arrive at Keel Mtn Preserve **1787 McMullen Rd, Gurley, AL 35748** at 10 AM.

If there are thunderstorms or the chance of rain exceeds 50% for the duration of the hike (10am-12pm) we will cancel and try again the following Sunday at the same time/place.

We will also be meeting once again the day after, 9/25, from 6-7 in MOR 145 where the topic will be Invasive Species.

Finally, on Sunday 10/15, we may be partnering with the Rock Climbing Club to help clean up the bouldering area at Rainbow Mountain, which also has some nice hiking.

I hope to see you there!!



IS IT PHISHING?

[External] Luna Physical Therapy is hiring for Patient Onboarding Associate-Call Center (part time hours) in Nashville, TN and 19 more new jobs



Your Indeed Job Feed <alert@indeed.com>
8/24/2023 8:42 PM



T [Redacted]@uah.edu



Your job feed for August 24, 2023

Jobs are based on your preferences, profile, and activity on Indeed ¹

Patient Onboarding Associate- Call Center (part time hours)

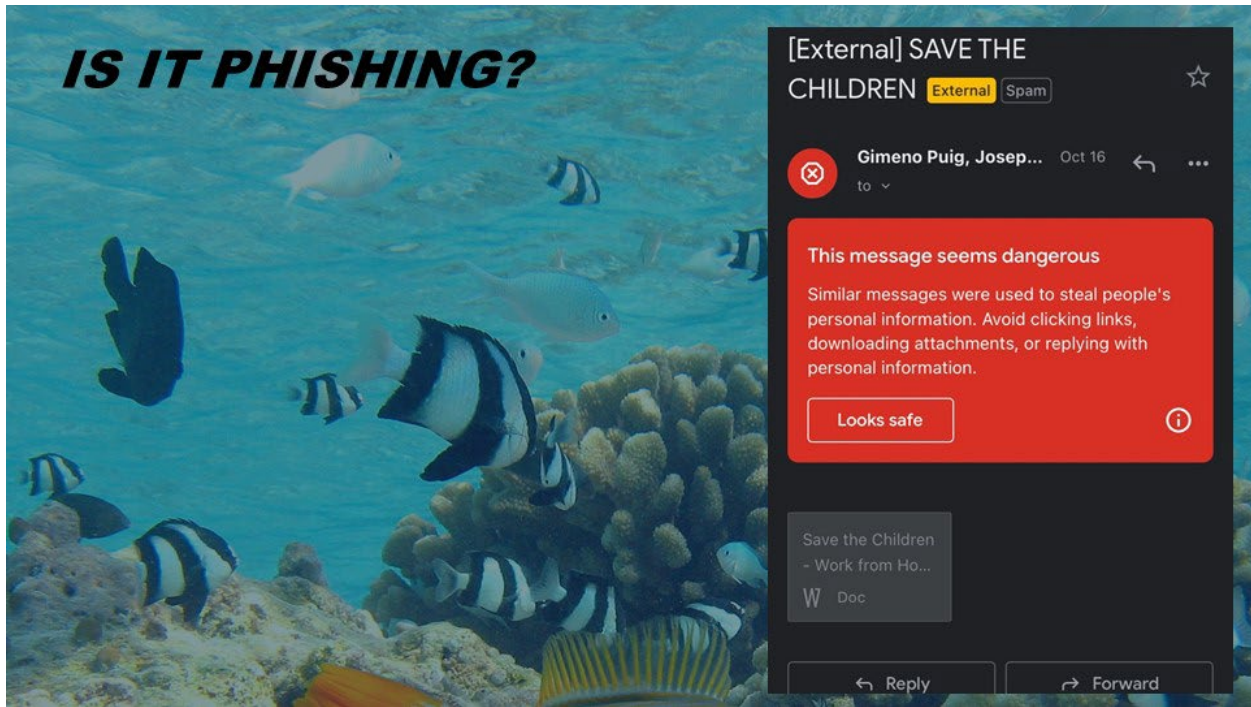
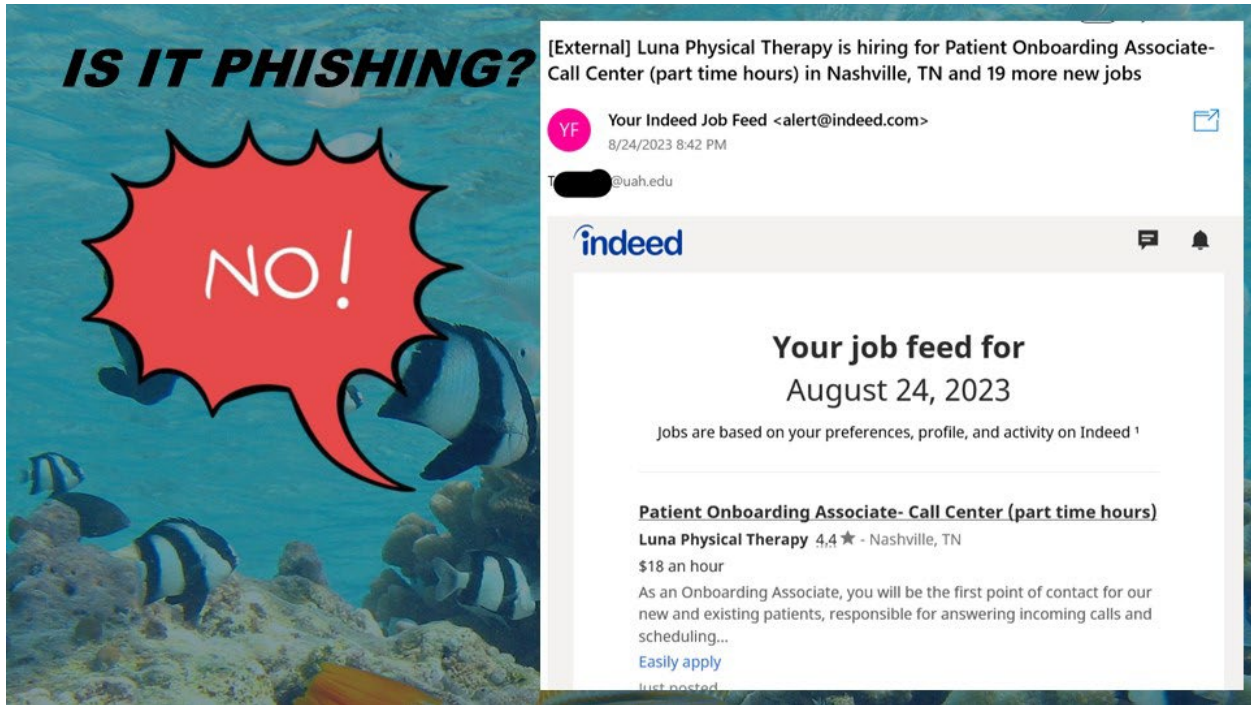
Luna Physical Therapy 4.4★ - Nashville, TN

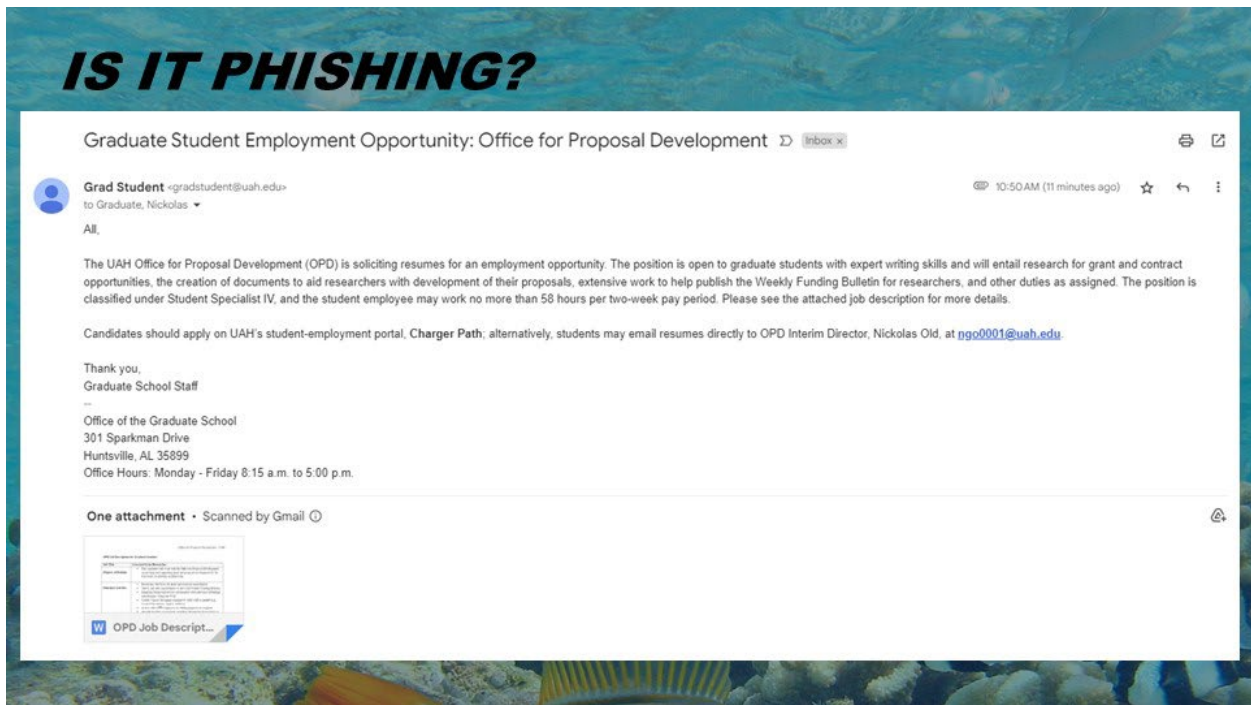
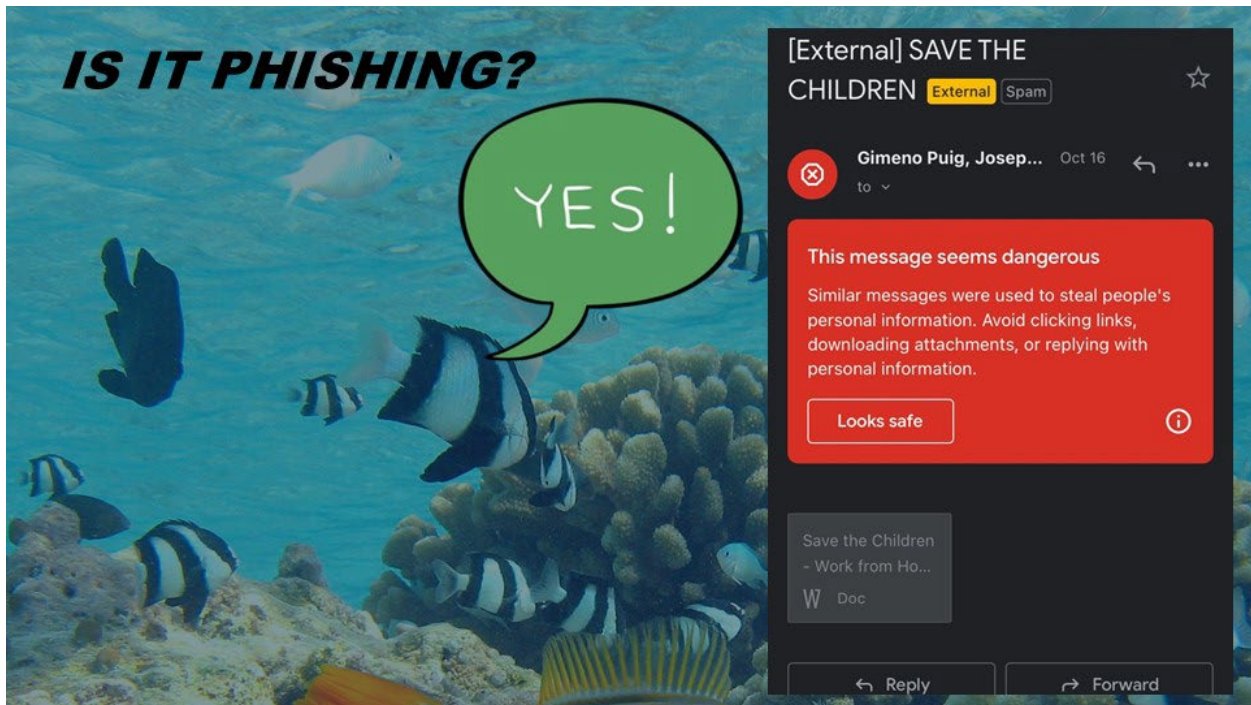
\$18 an hour

As an Onboarding Associate, you will be the first point of contact for our new and existing patients, responsible for answering incoming calls and scheduling...

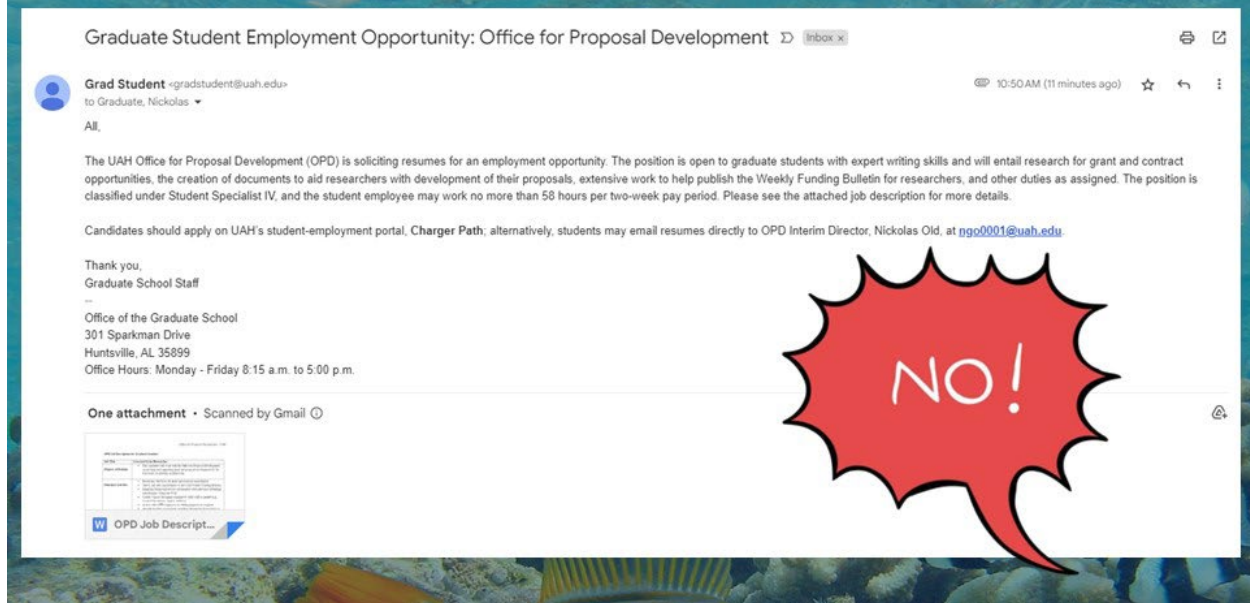
[Easily apply](#)

Just posted





IS IT PHISHING?



Graduate Student Employment Opportunity: Office for Proposal Development

Grad Student <gradstudent@uah.edu>
to Graduate, Nickolas

10:50 AM (11 minutes ago)

All

The UAH Office for Proposal Development (OPD) is soliciting resumes for an employment opportunity. The position is open to graduate students with expert writing skills and will entail research for grant and contract opportunities, the creation of documents to aid researchers with development of their proposals, extensive work to help publish the Weekly Funding Bulletin for researchers, and other duties as assigned. The position is classified under Student Specialist IV, and the student employee may work no more than 58 hours per two-week pay period. Please see the attached job description for more details.

Candidates should apply on UAH's student-employment portal, **Charger Path**; alternatively, students may email resumes directly to OPD Interim Director, Nickolas Old, at ngo0001@uah.edu.

Thank you,
Graduate School Staff

Office of the Graduate School
301 Sparkman Drive
Huntsville, AL 35899
Office Hours: Monday - Friday 8:15 a.m. to 5:00 p.m.

One attachment • Scanned by Gmail

OPD Job Descript...

NO!

So, what?

What should you do if you suspect an email you have received is a phishing attempt?

How to Report Phishing Emails

If you're using a work or school email, send them to whoever manages your cybersecurity.

At UAH, there is a button in the top right corner of every email where users can select "Report Phishing."

How to Report Phishing Emails

Report to your email provider that an email is phishing.

Report to the Internet Crime Complaint Center, which is managed by the FBI (<https://www.ic3.gov/>).



In your world...

what are some examples of phishing?



Phishing IRL

As a group, identify real world examples of phishing and how it impacts real businesses. Tell me how you knew that this was a phishing attempt and any damage caused.

Phishing IRL

Compare your examples.

What is similar? What is different?

Let's try it

come up with a phishing scheme

How to phish

Write a phishing email! Determine what and how you will phish and if you will spear phish or whale.

Identify the ways someone might know that you are attempting to phish them.





SO...



SO...

what is phishing?



SO...

what is phishing?
does it involve fish?

Sources

<https://www.investopedia.com/terms/p/personally-identifiable-information-pii.asp>

Vishing Slide Deck:

What is Vishing?

On a sheet of paper, describe vishing in a few sentences.



An Intro to Vishing and Social Engineering



Sarah Foltz

What is Vishing?

Vishing is similar to phishing in that the attacker is trying to gain access to victim's PII.

What is Vishing?

Vishing is similar to phishing in that the attacker is trying to gain access to victim's PII.

Instead of trying to attack over email, Vishing is done over phone calls or voice mail.

What is Vishing?

Vishing is similar to phishing in that the attacker is trying to gain access to victim's PII.

Instead of trying to attack over email, Vishing is done over phone calls or voice mail.

Attackers can spoof their voices (with modifiers or AI).

What is Vishing?

Vishing is similar to phishing in that the attacker is trying to gain access to victim's PII.

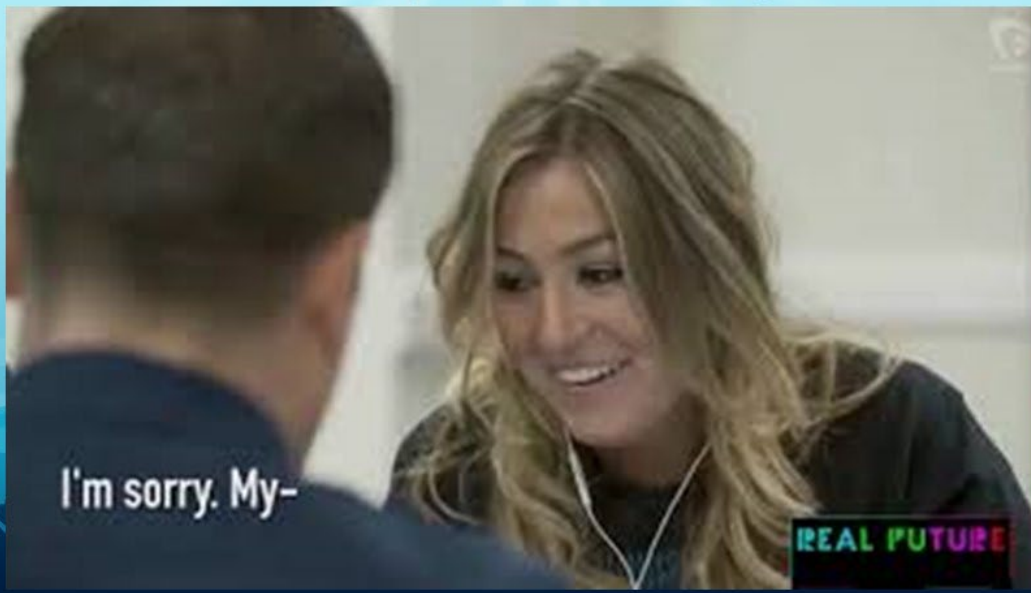
Instead of trying to attack over email, Vishing is done over phone calls or voice mail.

Attackers can spoof their voices (with modifiers or AI).

How does Vishing relate to Social Engineering?



Examples of Vishing



Examples of Vishing

 My grandmother was almost Vished!

Examples of Vishing

-  My grandmother was almost Vished!
-  Printer model

Examples of Vishing

- 📞 My grandmother was almost Vished!
- 📞 Printer model
- 📞 Say Yes to Confirm

Vishing Conversation!

Pretext: You are acting as a bank! The “bank” is trying to find some information about the victim.

Victim: You are receiving a call from someone claiming to be your bank. How do you respond?

How To Identify Vishing

- 📞 The visher acts like a someone you have not recently contacted
- 📞 The visher creates urgency
- 📞 The visher asks for PII
- 📞 The visher uses deliberately false statements
- 📞 The visher uses strong emotions
- 📞 The visher uses a quid pro quo
- 📞 The visher uses mumbling

Vishing Trivia!

- 📞 How much money did Americans lose in 2021 from phone scams?

Vishing Trivia!

- 🎯 How much money did Americans lose in 2021 from phone scams?
- 🎯 \$29,800,000.00

Vishing Trivia!

- 🎯 How much money did Americans lose in 2021 from phone scams?
- 🎯 Which companies are impersonated most often?
- 🎯 Who would companies be concerned about being vished?

Vishing Trivia!

- 🎧 How much money did Americans lose in 2021 from phone scams?
- 🎧 Which companies are impersonated most often?

Vishing Trivia!

- 🎧 How much money did Americans lose in 2021 from phone scams?
- 🎧 \$29,800,000.00
- 🎧 Which companies are impersonated most often?
- 🎧 Apple and Microsoft
- 🎧 Who would companies be concerned about being vished?

Vishing Trivia!

- How much money did Americans lose in 2021 from phone scams?
- \$29,800,000.00
- Which companies are impersonated most often?
- Apple and Microsoft
- Who would companies be concerned about being vished?
- HR, Sales, and Customer Service

Dangers of Vishing



What is Vishing?

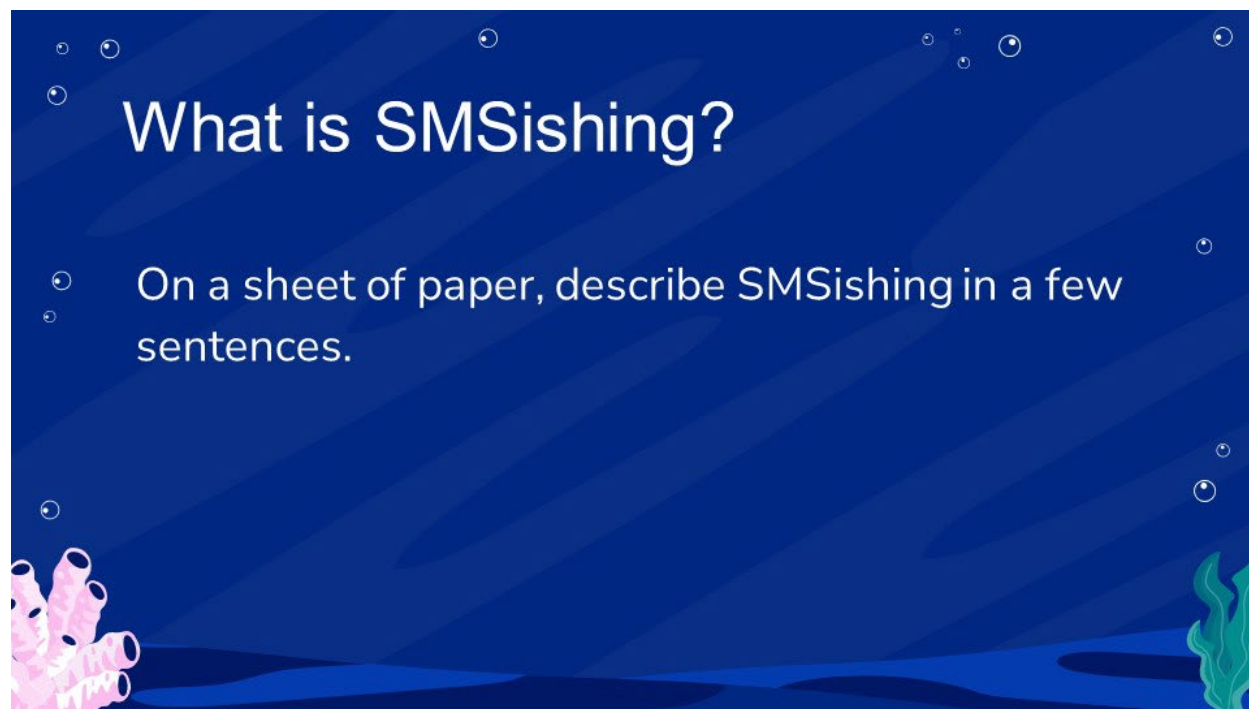
An underwater scene with a blue gradient background. Sunbeams of light stream down from the top. The bottom is dark with silhouettes of coral, rocks, and several fish swimming.

Sources

<https://www.social-engineer.org/framework/attack-vectors/vishing/>

An underwater scene with a blue gradient background. Sunbeams of light stream down from the top. The bottom is dark with silhouettes of coral, rocks, and several fish swimming.

SMSishing Slide Deck:



What is SMSishing?

- On a sheet of paper, describe SMSishing in a few sentences.

This slide features a dark blue background with a wavy pattern at the bottom, suggesting an underwater scene. There are several white circles of varying sizes scattered across the top and right sides, resembling bubbles. On the left side, there is a pink, branching coral-like structure. On the right side, there is a green, leafy seaweed-like structure.



An Introduction to
SMShing in Social
Engineering

Sarah Foltz

This slide features a dark blue background with a wavy pattern at the bottom, suggesting an underwater scene. There are several white circles of varying sizes scattered across the top and left sides, resembling bubbles. The title text is enclosed in a white rectangular box.

What is SMSishing?



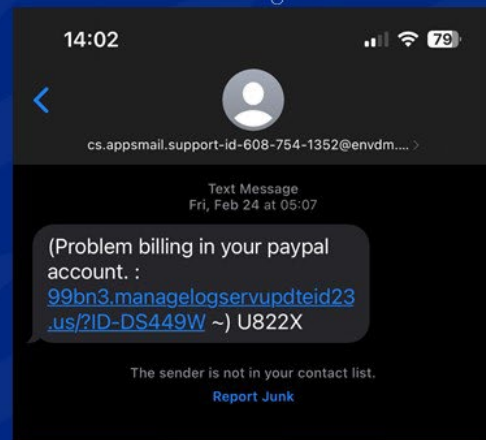
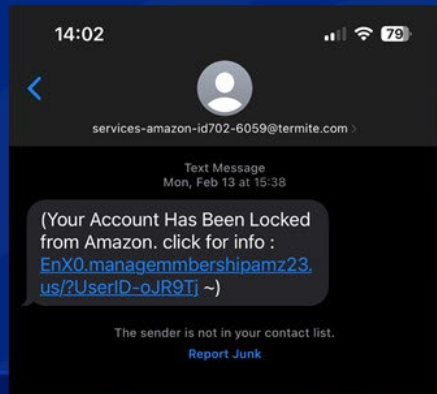
What is SMSishing?

SMSishing is sending fraudulent messages with the intent to capture Personally Identifiable Information (PII).



How Does SMSishing Relate to Social Engineering?

SMShing Examples





How do you know if a text is SMShing?

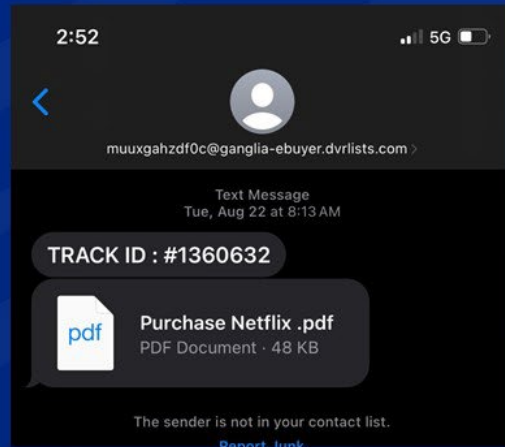


How do you know if a text is SMShing?

- An unexpected link
- An unexpected file
- An urgent request for money
- Winning a contest you did not enter
- You don't recognize the brand
- An urgent request for you to verify personal information via a link or automated phone number

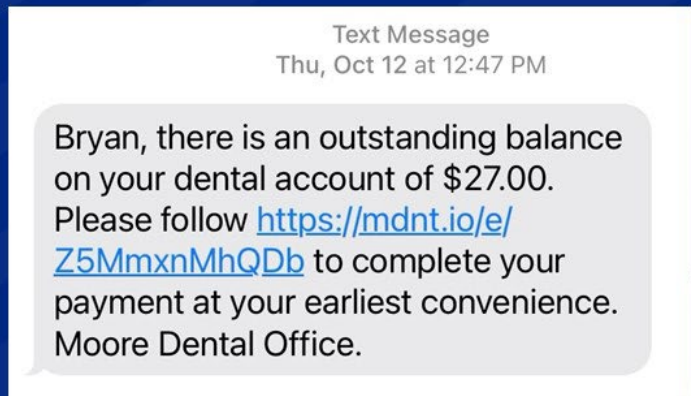
Real or SMShing?

SMSHING!



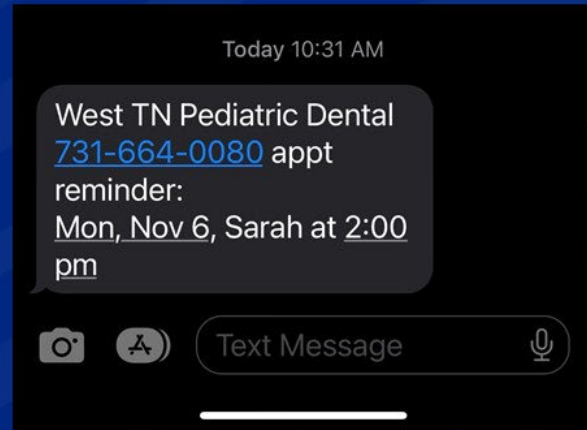
Real or SMShing?

Real!



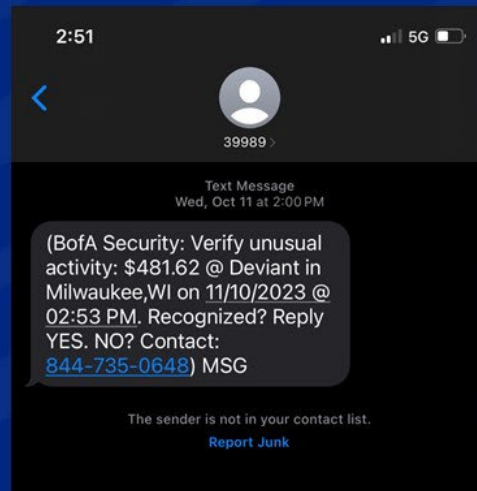
Real or SMShing?

Real!



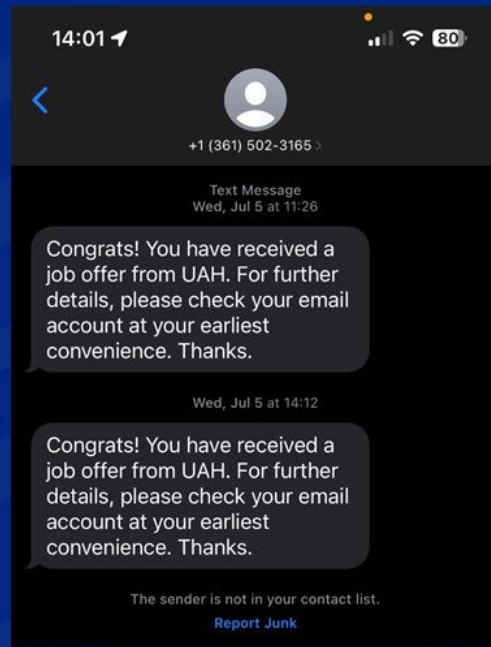
Real or SMShing?

SMShing!



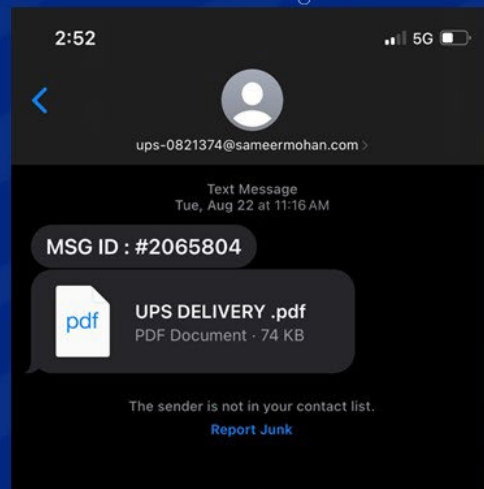
Real or SMShing?

Real!



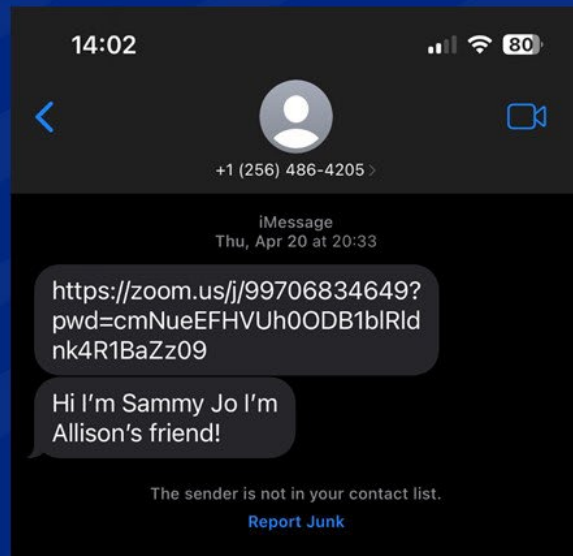
Real or SMShing?

SMShing!



Real or SMShing?

Real!



What danger does SMShing pose?

"The Federal Trade Commission logged over 93,000 complaints about unwanted text messages in 2018.

This included a 30% increase in smishing attempts from the previous year. In late 2018, about 125 Fifth Third Bank customers fell victim to a smishing scam.

They were all sent smishing text messages that tricked them into sharing their usernames and passwords. Over \$100,000 was stolen from the victims via ATMs, simply by using the information they provided." -<https://avira.com/en/blog/how-to-recognize-a-smishing-text-message>

How To Report SMShing

Forward the text to 7726 (this spells spam).

You will then receive a message asking what number the text came from.

Find Examples of SMShing As A Group!



What Are Some Common Elements
In The Messages You Found?



Write An Example Of A SMSishing
Attack

Recap

What is SMShing?

Sources

<https://www.social-engineer.org/framework/attack-vectors/vishing/>

<https://avira.com/en/blog/how-to-recognize-a-smishing-text-message>

Phishing Teaching Guide:

Intro

This teaching guide is to accompany the presentation, “An Introduction to Phishing in Social Engineering”. This presentation instructs students on what phishing is, how it relates to social engineering, how to identify it, and how to report it.

How to use this teaching guide

The slides are broken down by section. Each Section has a different time estimate. Slide numbers will be listed followed by a colon. Then, an explanation of what is happening on that slide follows. Sometimes, information for the discussion as background information will be in this section. The bullet points are what should be discussed with the class.

Section one: 15-20 min

Slide one:

What is phishing bell assignment

- Students will fill out what they think phishing is on a piece of paper while waiting for class to start.

Slide two:

Introduction.

- Explain that we are talking about Phishing.

Slide three:

Discussion

- Lead students in a discussion about what they think phishing is.

Slides four and five:

This slide explains what phishing is.

- Discuss with the class what phishing is and that it does not involve fish.

Slide six:

This slide defines phishing.

- Phishing is an email attack where attackers pose as fraudulent people or companies and try to obtain PII or convince a victim to install malware.

Slide seven:

Highlights PII to transition to PII discussion.

- Explain what PII is

Slide eight:

- Ask students to give examples of PII.

Slide nine:

Show examples of PII.

- Go through PII examples. Explain there are more PII's.

Slide ten:

Class discussion of what social engineering is Social engineering is deceiving individuals into divulging PII that may be used for fraudulent purposes.

- Have class define social engineering.

Side eleven:

Social engineering is trying to have people do what you want them to do without them thinking about it. Phishing is when attackers are attempting to have you provide PII without thinking about it

- Have class discuss how phishing is related to social engineering

Slides twelve-fifteen:

These slides provide different examples of phishing. The slides with images are real phishing emails friends or I received. The third slide is phish bowls. Phish bowls are collections of phishing emails that have been reported to universities. Many universities have phishbowls. Phishbowls help provide students with more examples of phishing.

- Talk the students through the phishing emails.
- Talk about phishbowls, and how they can serve as a useful resource.

Slides sixteen-eighteen:

These slides explain spear phishing and whaling.

- Explain that spear phishing targets a specific person. For example, a spear phishing attack may specifically target the principal of your high school.
- A whaling attack specifically targets a high-level person. For example, a whaling attack might target Bill Gates or Elon Musk.
- Both of these attacks will be tailored to the person they are targeting.

Slides 19-22:

Slide 19 talks about how to spot phishing attacks. 20 and 22 are the same phishing examples from earlier but with the common phishing markers highlighted.

- Have students provide common evidence of phishing.
- Go through the common phishing signifiers.
- Talk students through the phishing emails from earlier. The phishing signifiers are in yellow. Discuss how these things identify these emails as phishing.

Section 2: 10 minutes

Slides 23-33:

Students will now play everyone's favorite game: Is it Phishing? Students will identify whether the emails on screen are phishing emails. As you click once, the email will show on the screen. If you click twice, the answer to whether or not something is phishing will show. Click again to move to the next email.

- Instruct students that they are playing Is It Phishing.
- Have students hold up thumbs up or thumbs down if they think a given slide is phishing.
- After each slide, discuss how to tell if the email is or is not phishing.

Slides 34-36:

These slides explain how to report a phishing attack.

- How do you report phishing attacks?
- Report to work, school, Internet service provider, or FBI

Section 3: 10 minutes

Slides 37-39:

These slides ask students to relate phishing to real world examples.

- Have students tell you about phishing they encountered.
- Have students work in a group to find examples of phishing attacks and how these attacks impacted real businesses.
- Have students discuss similarities and differences between these phishing attacks

Section 4: 10 minutes or homework

Slides 40-41:

Students will practice these skills by writing their own phishing attacks.

- Have students write a phishing attack.
- Have them decide whether to spear, whale, or normal phish.
- Have them consider some of the common threads they saw in the real phishing attacks.

Slide 42:

- If time, watch a video about phishing In Real Life

Section 5: 3 minutes

Slides 43-45:

Wrap up.

- Have the class tell you what phishing is.

Slide 46:

Sources

Vishing Teaching Guide:

Intro

This teaching guide is to accompany the presentation, “An Introduction to Vishing in Social Engineering”. This presentation instructs students on what phishing is, how it relates to social engineering, and how to identify it.

How to use this teaching guide

The slides are broken down by section. Each Section has a different time estimate. Slide numbers will be listed followed by a colon. Then, an explanation of what is happening on that slide follows. Sometimes, information for the discussion as background information will be in this section. The bullet points are what should be discussed with the class.

Section one: 25 minutes

Slide one:

What is vishing bell assignment

- Students will fill out what they think vishing is on a piece of paper while waiting for class to start.

Slide two:

Introduction.

- Explain that we are talking about vishing.

Slides three-six:

Discussion. Vishing is similar to phishing, except it is done with voice. This can be done with AI or over the phone. The visher could also do it by leaving a voicemail. Phishing is looking for PII.

- Lead students in a discussion about what they think vishing is.
- Review PII.

Slides seven and eight:

Vishing relates to social engineering in a similar way to phishing. Vishing attacks attempt to have victims give up pii or send them money over the phone.

- Have students discuss vishing and how it relates to social engineering.
- Then play the video of social engineering and vishing.

Slides nine-eleven:

These slides provide examples of social engineering.

- My grandmother was almost vished. My grandmother received a call that my brother had snuck out of the house, caught a taxi to help a friend and ended up in jail. The caller was posing as “her grandson”. My grandmother responded, “Jacob?” She was very confused and concerned. She almost gave him money for his bail. Thankfully, she thought to call my father. My dad is an Information Systems professor. He explained that this was a vishing attack. My dad then reminded her that one, Jacob was at camp, and two, the small town we were in did not have taxis.
- Printer model. The university my dad works for, UTM regularly has people who receive calls claiming to be IT. They ask for all sorts of computer information and specs. They explain a problem with the printer that can only be solved with these expensive ink cartridges. The visher then proceeds to try and sell said ink cartridges. If people fall for it, then the university ends up being charged for these ink cartridges.

- Say yes to confirm. Several years ago, there was a vishing scam where vishers would call people and attempt to get them to say yes. So they would say “is this (victim name), and the victim would respond yes. The visher would record the victim saying yes. Then the attacker would play a sound saying do you confirm a purchase? And then play the recorded yes. The attacker would then get the victim to give card information to pay for whatever they agreed to purchase.

Section 2: 20 minutes

Slide 12:

Have a practice vishing conversation. One person pretends to be a bank. They are looking for the “victim”’s middle name.

- Have 2 students run a fake vishing conversation. The “bank” seeks the “victim’s” middle name. The “victim” must determine if this is a real vishing attack.

Slide 13:

Discuss how to determine if something is a vishing call.

- Go through the different ways students can tell if something is a vishing call.

Slides 14-19:

These slides have vishing trivia.

- Go through vishing trivia with students.
- Let students guess the answers.

Slide 20:

Slide 20 is a video showing the dangers of vishing.

- Watch video

Section 3: 5 minutes

Slides 21-22:

Review what phishing is.

SMSishing Teaching Guide:

Intro

This teaching guide is to accompany the presentation, “An Introduction to SMSishing in Social Engineering”. This presentation instructs students on what phishing is, how it relates to social engineering, how to identify it, and how to report it.

How to use this teaching guide

The slides are broken down by section. Each Section has a different time estimate. Slide numbers will be listed followed by a colon. Then, an explanation of what is happening on that slide follows. Sometimes, information for the discussion as background information will be in this section. The bullet points are what should be discussed with the class.

Section one: 20 minutes

Slide one:

What is SMSishing bell assignment

- Students will fill out what they think SMSishing is on a piece of paper while waiting for class to start.

Slide two:

Introduction.

- Explain that we are talking about SMSishing.

Slides three-four:

SMSishing is sending fraudulent messages with the intent to capture Personally Identifiable Information (PII).

- Discuss what SMSishing is.
- Review PII

Slide five:

- Have students explain how SMSishing relates to social engineering

Slide six:

This slide has 2 different text examples of SMSishing.

- Show SMSishing examples.

Slides seven-eight:

These slides show how to identify SMSishing.

- Have students suggest how to identify SMSishing.
- Show and go through how to identify SMSishing.

Section 2 20 minutes

Slides nine-fifteen:

This is everyone’s favorite game: Is It SMSishing?. Click once and the text appears. Click twice for the answer.

- Explain that we are playing Is It SMSishing.
- Students will get 10-15 seconds to read each text and decide if it is SMSishing.
- Have students hold up a thumb up if it is SMSishing and a thumb down if it is not SMSishing.
- Go through all of these slides.

Slide 16:

- Talk about the dangers of SMSishing.

Slide 17:

- Explain how to report SMSishing,

Slide 18:

- Have students work in a group to find real examples of SMSishing,

Slide 19:

- Have students discuss common elements between SMSishing attacks.

Slide 20:

- Have students write an example of an SMSishing message.

Section 3: 5 minutes

Slides 21 and 22:

- Have students recap what SMSishing is.
- Citations.

Assessment:

Name: _____

Date: _____

Phishing, Vishing, and SMSishing Quiz

1. What is phishing?
 - a. When fraudulent emails from seemingly reputable companies or people who ask for Personally Identifiable Information (PII) for nefarious purposes.
 - b. Sending fraudulent messages via text with the intent to capture Personally Identifiable Information.
 - c. Attempting to gain PII over voicemail.
 - d. Attempting to acquire fish.

2. What is vishing?
 - a. When fraudulent emails from seemingly-reputable companies or people who ask for Personally Identifiable Information (PII) for nefarious purposes.
 - b. Sending fraudulent messages via text with the intent to capture Personally Identifiable Information.
 - c. Attempting to gain PII over voicemail.
 - d. Attempting to acquire fish.

3. What is SMSishing?
 - a. When fraudulent emails from seemingly-reputable companies or people who ask for Personally Identifiable Information (PII) for nefarious purposes
 - b. Sending fraudulent messages via text with the intent to capture Personally Identifiable Information.
 - c. Attempting to gain PII over voicemail
 - d. Attempting to acquire fish

4. How do you report a SMSishing attack (**select all that apply**)?
 - a. If you're using a work or school email, send it to whoever manages your cybersecurity.
 - b. Forward the text to 7726 (this spells spam). You will then receive a message asking what number the text came from.
 - c. Report to your email provider that an email is phishing.

5. How do you report a Phishing attack (**select all that apply**)?
 - a. If you're using a work or school email, send it to whoever manages your cybersecurity.
 - b. Forward the text to 7726 (this spells spam). You will then receive a message asking what number the text came from.
 - c. Report to your email provider that an email is phishing.

6. What is whaling?
 - a. Fishing for whales
 - b. Trying to phish a specific person
 - c. Trying to phish a high-level specific person
 - d. Trying to phish someone over voicemail

7. What is spearphishing?
 - a. Fishing for whales
 - b. Trying to phish a specific person
 - c. Trying to phish a high-level specific person
 - d. Trying to phish someone over voicemail

8. How do you identify SMSishing (**select all that apply**)?
 - a. It comes from a friend.
 - b. An urgent request for you to verify personal information via a link or automated phone number.
 - c. It contains a suspicious link.
 - d. It says you won a contest you did not enter.

9. How much money did Americans lose in 2021 from phone scams?
 - a. \$29,800,000
 - b. \$1,000,000
 - c. \$20,000,000
 - d. \$37,000,000

10. How do you identify vishing?
 - a. The visher uses deliberately false statements.
 - b. The visher acts like someone you have not recently contacted.
 - c. The visher uses a quid pro quo.
 - d. All of the above.

11. How do you identify phishing (**Select all that apply**)?
 - a. Wrong email addresses
 - b. Does not make sense for this person to email you
 - c. Tries to make you click a link
 - d. Correct grammar and spelling

12. Which of the following is not PII?
 - a. Drivers License Number
 - b. Social Security Number
 - c. Passport Number
 - d. First Name

13. Write a SMSishing message.

14. How do phishing, SMSishing, and vishing relate to social engineering?

15. Where can you find examples of phishing?

Answer Key: (Answers are highlighted and have an asterisk at the end of the answer)

Name: _____
Date: _____

Phishing, Vishing, and SMSishing Quiz Answer Guide

1. What is phishing?
 - a. When fraudulent emails from seemingly reputable companies or people who ask for Personally Identifiable Information (PII) for nefarious purposes.*
 - b. Sending fraudulent messages via text with the intent to capture Personally Identifiable Information.
 - c. Attempting to gain PII over voicemail.
 - d. Attempting to acquire fish.
2. What is vishing?
 - a. When fraudulent emails from seemingly-reputable companies or people who ask for Personally Identifiable Information (PII) for nefarious purposes.
 - b. Sending fraudulent messages via text with the intent to capture Personally Identifiable Information.
 - c. Attempting to gain PII over voicemail.*
 - d. Attempting to acquire fish.
3. What is SMSishing?
 - a. When fraudulent emails from seemingly-reputable companies or people who ask for Personally Identifiable Information (PII) for nefarious purposes
 - b. Sending fraudulent messages via text with the intent to capture Personally Identifiable Information.*
 - c. Attempting to gain PII over voicemail
 - d. Attempting to acquire fish
4. How do you report a SMSishing attack (select all that apply)?
 - a. If you're using a work or school email, send it to whoever manages your cybersecurity.
 - b. Forward the text to 7726 (this spells spam). You will then receive a message asking what number the text came from.*
 - c. Report to your email provider that an email is phishing.
5. How do you report a Phishing attack (select all that apply)?
 - a. If you're using a work or school email, send it to whoever manages your cybersecurity.*

- b. Forward the text to 7726 (this spells spam). You will then receive a message asking what number the text came from.
 - c. Report to your email provider that an email is phishing.*
6. What is whaling?
- a. Fishing for whales
 - b. Trying to phish a specific person
 - c. Trying to phish a high-level specific person*
 - d. Trying to phish someone over voicemail
7. What is spearphishing?
- a. Fishing for whales
 - b. Trying to phish a specific person
 - c. Trying to phish a high-level specific person
 - d. Trying to phish someone over voicemail
8. How do you identify SMSishing (select all that apply)?
- a. It comes from a friend
 - b. An urgent request for you to verify personal information via a link or automated phone number.*
 - c. It contains a suspicious link.*
 - d. It says you won a contest you did not enter.*
9. How much money did Americans lose in 2021 from phone scams?
- a. \$29,800,000*
 - b. \$1,000,000
 - c. \$20,000,000
 - d. \$37,000,000
10. How do you identify vishing?
- a. The visher uses deliberately false statements.
 - b. The visher acts like someone you have not recently contacted.
 - c. The visher uses a quid pro quo.
 - d. All of the above.*
11. How do you identify phishing (Select all that apply)?
- a. Wrong email addresses*
 - b. Does not make sense for this person to email you*
 - c. Tries to make you click a link*
 - d. Correct grammar and spelling
12. Which of the following is not PII?
- a. Drivers License Number
 - b. Social Security Number
 - c. Passport Number
 - d. First Name*

13. Write a SMSishing message.

Any acceptable SMSishing message. For example: Your package has been delivered. Please click here: tinyurl.com/asdfih2408hf08hwroh.

14. How do phishing, SMSishing, and vishing relate to social engineering?

Any similar answer is correct : Social Engineering involves tricking people into providing personal information that can be used for fraud. Phishing, vishing, and smishing are all examples of people using social engineering through email, voicemail, and texting to gain personal information.

15. Where can you find examples of phishing?

Any place where someone could find phishing examples is acceptable. For example, phish bowls, the internet, in work training courses.

Bibliography:

Avira. (2022, July 12). *How to recognize smishing attacks and avoid becoming a victim*. Avira Blog. <https://avira.com/en/blog/how-to-recognize-a-smishing-text-message>

Dr. Hovermale's Social Engineering Class, Fall 2023

Frankenfield, J. (n.d.). *What is personally identifiable information (PII)? types and examples*.

Investopedia. <https://www.investopedia.com/terms/p/personally-identifiable-information-pii.asp>

Ikeda, E. (2023, March 30). *Ai can replicate voices in high-tech phone call scams, FTC warns*.

YouTube.

https://www.youtube.com/watch?v=V6_jCGzR020&embeds_referring_euri=https%3A%2F%2Fdocs.google.com%2F&embeds_referring_origin=https%3A%2F%2Fdocs.google.com&source_ve_path=MjM4NTE&feature=emb_title

Myler, G. (2018, May 15). *Social Engineering: Vishing example*. YouTube.

https://www.youtube.com/watch?v=xuYoMs6CLEw&embeds_referring_euri=https%3A%2F%2Fdocs.google.com%2F&embeds_referring_origin=https%3A%2F%2Fdocs.google.com&source_ve_path=MzY4NDIsMjM4NTE&feature=emb_title

Vishing. Security Through Education. (2022, May 31).

<https://www.social-engineer.org/framework/attack-vectors/vishing/>